Práctica Profesional

Estrategia de preparación institucional en ciberdiplomacia para el Ministerio de Relaciones Exteriores de Colombia.

Yuliana Villarraga Cano

Programa de Administración Pública

Práctica realizada en el Ministerio de Relaciones Exteriores de Colombia

Dirección de Europa – GIT de Europa Occidental y Asuntos ante la Unión Europea

Asesora: Shannon Rey Cadavid

Escuela Superior de Administración Pública

Bogotá D.C

2025

Agradecimientos

A mi familia, mi pareja y mis amigos, por su compañía, paciencia y constante apoyo.

A la Escuela Superior de Administración Pública, por brindarme las herramientas para crecer profesionalmente.

Y al Ministerio de Relaciones Exteriores, por brindarme un espacio de aprendizaje profesional.

Resumen

La presente monografía se desarrolla en el marco de la práctica profesional realizada en el Ministerio de Relaciones Exteriores de Colombia, específicamente en el Grupo Interno de Trabajo de Europa Occidental y Asuntos ante la Unión Europea. A partir de esta experiencia, se plantea un análisis sobre la necesidad de incorporar la ciberdiplomacia como eje estratégico de acción exterior frente al creciente riesgo de amenazas digitales. En ese sentido, el trabajo propone un enfoque preventivo que articule la gestión de la seguridad digital con los lineamientos de la política exterior colombiana. Se examina el desarrollo normativo nacional en materia de seguridad digital y su desconexión con los instrumentos diplomáticos actuales, lo cual representa una oportunidad para el fortalecimiento institucional. Además, se incluyen antecedentes internacionales —como los casos de Letonia y Albania— que evidencian la importancia de una diplomacia activa en ciberseguridad. El producto final consiste en la formulación conceptual de una estrategia interna que vincule acciones como sensibilización, formación técnica, coordinación interinstitucional y participación en foros multilaterales. Finalmente, se emplea un análisis prospectivo para identificar posibles escenarios y recomendaciones para la Cancillería, con el fin de posicionar a Colombia en la gobernanza digital global.

Palabras clave.

ciberdiplomacia, seguridad digital, inteligencia artificial, relaciones internacionales, política exterior colombiana.

Índice

Lista de tablas

Introducción

La presente monografía se desarrolla en el marco de la práctica administrativa realizada en el Ministerio de Relaciones Exteriores de Colombia, específicamente en el Grupo Interno de Trabajo de Europa Occidental y Asuntos ante la Unión Europea, adscrito a la Dirección de Europa. Esta dependencia tiene como misión principal fortalecer las relaciones bilaterales de Colombia con los países de Europa Occidental y con las instituciones de la Unión Europea, mediante la formulación de estrategias políticas, económicas, sociales y culturales que respondan a los intereses nacionales en el escenario internacional.

Uno de los principales desafíos que enfrenta actualmente la Cancillería colombiana es su capacidad institucional para anticipar y responder a riesgos emergentes en el ciberespacio, como ciberataques a infraestructuras críticas, manipulación de datos, campañas de desinformación y conflictos digitales que afectan directamente la política exterior. La evolución de las amenazas digitales ha llevado a que el ciberespacio sea considerado una nueva dimensión de la seguridad internacional, lo cual exige la incorporación de la ciberdiplomacia como herramienta estratégica dentro de la acción exterior del Estado.

En este contexto, se ha identificado la necesidad de fortalecer los mecanismos institucionales de prevención estratégica y gobernanza digital, a partir de experiencias internacionales recientes. El caso de Albania, víctima en 2022 de un ciberataque atribuido a un actor estatal, obligó al país a romper relaciones diplomáticas y generó un llamado global a reforzar la cooperación cibernética. Por su parte, Letonia y Estonia han avanzado en la consolidación de políticas públicas de ciberseguridad y diplomacia digital en el marco de la OTAN y la Unión Europea, convirtiéndose en referentes regionales en el desarrollo de capacidades diplomáticas frente a amenazas híbridas. (Christou, 2015) (Kurbalija, 2016)

Estas experiencias internacionales evidencian que la preparación institucional frente a los riesgos digitales no puede ser reactiva, sino anticipatoria, intersectorial y diplomáticamente articulada. Desde la perspectiva de la administración pública, esto se alinea con los postulados de la Nueva Gestión Pública, que promueve modelos de gestión orientados a resultados, innovación tecnológica y adaptación organizacional (CLAD, 1998), así como con los principios del Gobierno Abierto, que abogan por la transparencia, la trazabilidad informativa y la colaboración multiactor en entornos digitales (OCDE, 2015).

En este sentido, la presente monografía propone una reflexión sobre el papel que debe asumir la Cancillería colombiana frente a los desafíos del entorno digital, a través del diseño conceptual de líneas de acción para la incorporación de la ciberdiplomacia como eje de política exterior preventiva. Esta iniciativa busca contribuir al fortalecimiento institucional del Ministerio y a la generación de capacidades técnicas y políticas para enfrentar con mayor resiliencia y legitimidad los riesgos que impone el nuevo orden internacional digital.

Objetivos

Objetivo general

Fortalecer las competencias en análisis político, gestión administrativa y relaciones internacionales mediante el apoyo en la formulación de informes, documentos estratégicos y actividades en la Coordinación de Europa Occidental y Asuntos ante la Unión Europea del Ministerio de Relaciones Exteriores, entendiendo el proceso de toma de decisiones y a la ejecución de estrategias diplomáticas.

Objetivos específicos

- Apoyar en la preparación de insumos estratégicos para reuniones de alto nivel.
- Sistematizar y actualizar bases de datos de noticias, perfiles diplomáticos y eventos relevantes.
- Elaborar documentos de análisis sobre contextos políticos y diplomáticos de Europa Occidental y de la Unión Europea.
- Analizar el papel de la inteligencia artificial y otras tecnologías emergentes como herramientas estratégicas para fortalecer la prevención, detección y gestión de riesgos digitales, así como para optimizar la toma de decisiones y la proyección internacional de Colombia en el marco de la ciberdiplomacia.

Descripción de la entidad

El Ministerio de Relaciones Exteriores de Colombia, también conocido en Colombia como la Cancillería, es la entidad del Estado encargada de formular, dirigir, coordinar y ejecutar la política exterior de la República de Colombia. Según lo establecido en el Decreto 869 de 2016, esta institución tiene la responsabilidad de representar al país en el ámbito internacional, promover

sus intereses, representar y proteger a los colombianos en el exterior (Ministerio de Relaciones Exteriores., 2016).

En palabras del propio decreto, "el Ministerio de Relaciones Exteriores de Colombia es la entidad encargada de formular, dirigir y ejecutar la política exterior de la República" (Ministerio de Relaciones Exteriores., 2016, pág. 2). Esta función posiciona al Ministerio como una entidad de planificación estratégica internacional, en el que la formulación y ejecución de políticas públicas transcienden el ámbito nacional. De esta manera, su actuar debe responder a los principios de eficiencia, eficacia y servicio al ciudadano, fundamentos esenciales de la Nueva Gestión Pública.

El Ministerio estructura sus funciones en varias direcciones, entre las cuales la Dirección de Europa, es la encargada de coordinar y ejecutar la política exterior de Colombia con los países del continente europeo. En particular, el GIT de Europa Occidental y Asuntos ante la Unión Europea se enfoca en fortalecer las relaciones bilaterales, apoyar en la cooperación económica, política y cultural, así como dar seguimiento a las relaciones políticas con los países de Europa Occidental y con las instituciones de la Unión Europea.

En un contexto de interdependencia global, desafíos como el cambio climático, el desarrollo sostenible y la gestión migratoria exigen una cooperación internacional más flexible, integrada e innovadora. Esto implica que entidades como el Ministerio de Relaciones Exteriores de Colombia asuman un papel activo en la generación de consensos y soluciones colectivas, superando los esquemas tradicionales y adoptando modelos de gobernanza pública que trasciendan las fronteras nacionales. (Ocampo, 2015).

El fortalecimiento de las relaciones bilaterales con Europa se ha convertido en un objetivo estratégico para Colombia, tanto para diversificar alianzas diplomáticas como para respaldar la paz total y el desarrollo sostenible. En un contexto de creciente vulnerabilidad ante amenazas digitales, la Comisión Europea y la *e-Governance Academy* han impulsado entrenamientos en ciberdiplomacia orientados a líderes y expertos, con el fin de reforzar capacidades estatales y promover una gobernanza digital internacional basada en principios democráticos y de cooperación.

Actividades realizadas

Durante el desarrollo de la práctica profesional en el Grupo Interno de Trabajo de Europa Occidental y Asuntos ante la Unión Europea del Ministerio de Relaciones Exteriores de Colombia, se han realizado diversas actividades que han contribuido significativamente al fortalecimiento de competencias propias de la administración pública, tales como la capacidad analítica, la gestión de la información, la coordinación interinstitucional y la formulación de insumos estratégicos.

1. Apoyo en la preparación de insumos para reuniones de alto nivel, se ha participado activamente en la elaboración de documentos de soporte para reuniones del Presidente de la República, la Canciller, los Viceministros y otras altas autoridades. Esta labor ha requerido el análisis de información diplomática, económica y política relevante, desarrollando habilidades de síntesis, redacción y priorización de información del ámbito internacional.
2. Investigación y elaboración de documentos de análisis de contexto político y económico de los países de Europa Occidental y de la Unión Europea. Esta actividad ha fortalecido la capacidad de análisis prospectivo y de comprensión de escenarios políticos, para así poder interpretar los entornos cambiantes como anticipar riesgos y oportunidades para el país.

3. Actualización de bases de datos de noticias, perfiles diplomáticos y embajadores para fortalecer las competencias en gestión documental, organización de datos estratégicos y manejo de herramientas digitales garantizando la trazabilidad de la información para una toma de decisiones informadas en la gestión estatal.
4. Participación en reuniones bilaterales y apoyo logístico en reuniones con delegaciones comerciales y diplomáticas, como las de Suiza, Noruega y Bélgica, ha proporcionado experiencia práctica en la interacción internacional, el seguimiento de acuerdos bilaterales, y la promoción de intereses nacionales. El apoyo logístico en eventos y actividades bilaterales también ha permitido comprender la importancia de la planeación y la coordinación efectiva entre diferentes entidades gubernamentales.
5. Elaboración de actas, memorias y documentos de apoyo para la Subcomisión Cultural y Educativa con España, desarrollando habilidades en sistematización de reuniones, redacción de memorias institucionales y seguimiento de compromisos, para lograr una correcta gestión administrativa.
6. Seguimiento a pronunciamientos de jefes de Estado y de Gobierno de Europa Occidental y la Unión Europea, reforzando la capacidad de observación crítica y de análisis de políticas exteriores comparadas, necesario para identificar tendencias globales y adaptar estrategias de política pública a contextos dinámicos e interdependientes.
7. Apoyo en la organización de la III reunión de consultas políticas entre Colombia e Irlanda, se brindó apoyo técnico y logístico desde el GIT de Europa, contribuyendo a la preparación de insumos estratégicos y al desarrollo del evento diplomático. Esta experiencia se vincula directamente con el enfoque de la administración pública orientada a resultados, ya que implicó coordinar acciones entre actores institucionales de alto nivel, organizar información

sensible y participar en procesos de toma de decisiones informadas. La cooperación con Irlanda giró en torno a temas como el proceso de paz, el fortalecimiento comercial y la migración laboral.

8. La participación en la reunión de consultas políticas entre Colombia y Francia representó una oportunidad significativa para aplicar competencias técnicas y analíticas en el marco de la administración pública internacional. El diálogo sobre inteligencia artificial y tecnología, en particular, pone de manifiesto la necesidad de una administración pública innovadora y adaptativa, en línea con los principios de la Nueva Gestión Pública y el Gobierno Abierto, que promueven el uso responsable de herramientas digitales y el diseño de políticas públicas basadas en datos. (OCDE, 2015)

Durante la práctica profesional se fortalecieron competencias clave de la administración pública, especialmente en lo relacionado con la formulación de políticas internacionales, la gestión estratégica del Estado y la articulación interinstitucional. La participación en las consultas políticas con países como Irlanda y Francia permitió aplicar habilidades de coordinación diplomática, planificación basada en consensos y seguimiento a compromisos bilaterales. Además, el apoyo en la preparación logística y la elaboración de documentos estratégicos puso en evidencia la importancia de capacidades como la redacción técnica, la organización de información y la comunicación efectiva en contextos diplomáticos. Estas actividades reflejan principios de la Nueva Gestión Pública, orientados a la eficiencia, los resultados y la incorporación de tecnologías como la inteligencia artificial, tema que también fue abordado en los diálogos internacionales.

Asimismo, la colaboración con entidades como ProColombia, Migración Colombia y otros ministerios evidenció una práctica de gobernanza multinivel, alineada con los enfoques de Gobierno Abierto y coordinación interinstitucional. Estas experiencias, además de permitir la

aplicación práctica del conocimiento académico, exigieron un alto grado de autonomía, análisis crítico y capacidad de adaptación. A lo largo del proceso, se afrontaron nuevos desafíos que impulsaron la iniciativa personal, el aprendizaje continuo y la mejora de habilidades técnicas, reafirmando la importancia de la formación práctica en escenarios reales de la gestión pública internacional.

Estrategia de preparación institucional en ciberdiplomacia para el Ministerio de Relaciones Exteriores de Colombia.

El producto final de la práctica consistirá en el planteamiento conceptual de una estrategia de preparación institucional en ciberdiplomacia, orientada a fortalecer la capacidad del Ministerio de Relaciones Exteriores, y en particular del Grupo Interno de Trabajo de Europa Occidental y Asuntos ante la Unión Europea, frente a los desafíos emergentes del entorno digital global.

Este planteamiento surge de una necesidad identificada durante el desarrollo de la práctica, particularmente a raíz de discusiones internas sostenidas en reuniones del GIT, donde se abordó la creciente relevancia de la ciberdiplomacia y los riesgos geopolíticos asociados al ciberespacio. En ese contexto, y gracias a la socialización de experiencias recientes como la participación de un funcionario en una conferencia internacional en Estonia —país referente en ciberseguridad y diplomacia digital—, se reconoció la importancia de que la Cancillería avance hacia un modelo preventivo, estratégico e interinstitucional frente a los conflictos y amenazas digitales.

La propuesta se enfocará en el desarrollo de líneas de acción institucionales que permitan anticipar, mitigar y gestionar riesgos digitales que puedan afectar las relaciones bilaterales, la imagen del Estado colombiano en el exterior, la seguridad de la información diplomática y la participación internacional en foros de gobernanza del ciberespacio.

Desde el campo de la administración pública, esta propuesta se fundamenta en los principios de la Nueva Gestión Pública, que promueve una administración eficiente, adaptativa y basada en resultados (CLAD, 1998), así como en los lineamientos del Gobierno Abierto, que busca garantizar la transparencia, la trazabilidad informacional y la innovación pública mediante el uso estratégico de tecnologías digitales (OCDE, 2015). La incorporación de la ciberdiplomacia dentro de la estrategia institucional se presenta como un paso necesario para consolidar una política exterior más resiliente, basada en inteligencia institucional, gobernanza tecnológica y alianzas digitales multilaterales.

Se espera que esta propuesta contribuya a:

- Reconocer y caracterizar los principales riesgos digitales que enfrentan las relaciones exteriores colombianas.
- Promover la integración de la ciberdiplomacia como línea estratégica dentro del accionar del Ministerio.
- Fomentar una cultura organizacional orientada a la prevención, la cooperación internacional y la transformación digital del servicio exterior.

Antecedentes

En las últimas dos décadas, la digitalización ha transformado las dinámicas del poder internacional y la forma en que los Estados se relacionan entre sí. El ciberespacio se ha consolidado como un nuevo escenario geopolítico donde convergen intereses diplomáticos, económicos, militares y sociales. Este entorno digital, altamente interconectado, ha generado oportunidades de cooperación, pero también ha expuesto a los Estados a nuevas formas de amenaza, como

ciberataques, desinformación, espionaje digital y manipulación de infraestructuras críticas (Kurbalija, 2016).

Uno de los casos más relevantes en la construcción de capacidades diplomáticas y de defensa en el entorno digital es el de Estonia, país que sufrió en 2007 uno de los primeros ciberataques masivos atribuidos a actores estatales. Este evento, que afectó servicios gubernamentales, financieros y de medios de comunicación, marcó un punto de inflexión en la comprensión global de la ciberseguridad como asunto de seguridad nacional y diplomática. En respuesta, Estonia no solo reforzó su infraestructura digital, sino que se posicionó como líder internacional en ciberdiplomacia, gobernanza de Internet y cooperación en ciberseguridad, siendo sede del Centro de Excelencia de la OTAN en Ciberdefensa (CCDCOE). (Ministry of Foreign of Republic of Estonia, 2024)

De manera más reciente, el caso de Albania evidenció la dimensión geopolítica del ciberespacio. En 2022, el gobierno albanés fue víctima de un ciberataque a gran escala dirigido contra sus servicios digitales clave, presuntamente ejecutado por actores vinculados al gobierno iraní. Este ataque llevó a la ruptura de relaciones diplomáticas, y generó una respuesta internacional coordinada, incluyendo asistencia técnica de aliados occidentales como Estados Unidos y apoyo político de la Unión Europea (Kavanagh, 2022).

Por su parte, Letonia ha desarrollado un enfoque integral en materia de seguridad digital y diplomacia tecnológica. A través de la colaboración con socios europeos y multilaterales, Letonia ha fortalecido su capacidad de ciberdefensa, promovido la diplomacia digital y aportado activamente a las discusiones normativas sobre ciberseguridad en foros como Naciones Unidas, la OSCE y el Consejo de Europa (Christou, 2015).

Estos tres casos evidencian que el ejercicio de la diplomacia moderna debe ir más allá de la representación formal y el diálogo tradicional entre Estados. La ciberdiplomacia, entendida como la articulación de herramientas diplomáticas, tecnológicas y jurídicas para proteger los intereses nacionales en el ciberespacio, se ha convertido en un campo estratégico de creciente relevancia (Kurbalija, 2016) (Nye, 2010).

En el contexto colombiano, si bien se han dado avances importantes en materia de transformación digital del Estado, aún se observa una limitada institucionalización de la ciberdiplomacia como componente formal de la política exterior. La rotación de personal en las direcciones, la ausencia de protocolos integrales de respuesta ante amenazas digitales en misiones diplomáticas, y la poca participación de Colombia en foros de gobernanza del ciberespacio, reflejan una oportunidad clave para el fortalecimiento de capacidades en esta materia. La práctica profesional desarrollada en el Grupo Interno de Trabajo de Europa Occidental y Asuntos ante la Unión Europea ha permitido identificar esta brecha, al tiempo que brinda una oportunidad para proponer lineamientos estratégicos que posicionen a la Cancillería frente a los desafíos del siglo XXI en materia de diplomacia digital.

Marco teórico.

La administración pública contemporánea enfrenta el desafío de adaptarse a un entorno global altamente interdependiente, caracterizado por transformaciones tecnológicas aceleradas, nuevas amenazas transnacionales y una ciudadanía cada vez más exigente en términos de transparencia, participación y eficiencia institucional. En este contexto, diversas corrientes teóricas han orientado la evolución del aparato estatal.

La Nueva Gestión Pública (NGP) es un enfoque administrativo que surgió en los años 80 como respuesta a las deficiencias del modelo burocrático clásico. Este paradigma promueve una

administración más eficiente, centrada en resultados, orientada al ciudadano, con estructuras más flexibles y con incorporación de herramientas del sector privado para mejorar la gestión estatal.

En América Latina, el (CLAD, 1998) propuso una versión contextualizada de la NGP, reconociendo la necesidad de fortalecer las capacidades del Estado sin renunciar al control democrático, la equidad y la legitimidad institucional. Bajo estos principios, la práctica profesional desarrollada en el Ministerio de Relaciones Exteriores se alinea con la idea de generar valor público mediante una gestión estratégica de la información, basada en evidencia y orientada a la toma de decisiones oportunas.

El Gobierno Abierto es un enfoque de gestión pública que promueve la transparencia, la participación ciudadana y la colaboración entre Estado y sociedad. Surge como parte de una evolución en la forma de gobernar, reconociendo que la legitimidad del Estado también se construye a partir de la confianza y del acceso a la información pública.

Según la (OCDE, 2015), los gobiernos deben garantizar que la información institucional sea accesible, reutilizable, comprensible y disponible digitalmente. En este marco, la implementación de estrategias digitales en la política exterior debe responder a criterios de trazabilidad, interoperabilidad y colaboración multiactor. La capacidad del Estado para anticipar y prevenir amenazas —como ciberataques, desinformación o brechas de ciberseguridad— también debe estar anclada en principios de apertura institucional y cooperación internacional.

La sistematización de información estratégica en el sector público consiste en organizar, estructurar, interpretar y documentar datos relevantes para la toma de decisiones, el aprendizaje institucional y la evaluación de políticas públicas. Esta herramienta es importante en contextos de

política exterior, donde el seguimiento a declaraciones, acuerdos, actores clave y contextos geopolíticos es fundamental.

Según (Ocampo, 2015), en un entorno internacional interdependiente, la información estratégica debe ser considerada como un bien público global. En este sentido, el fortalecimiento institucional para gestionar esa información es una condición necesaria para la acción estatal eficaz. La pérdida de información por alta rotación institucional —como ocurre en el servicio exterior— representa un riesgo que puede mitigarse mediante estructuras digitales que faciliten la continuidad de la gestión y la memoria institucional.

La diplomacia es el conjunto de estrategias mediante las cuales un Estado busca influir en otros países, promover su imagen internacional, mostrar su importancia en el ámbito internacional y fortalecer vínculos bilaterales o multilaterales. Ya no es solo una diplomacia tradicional, que se centraba en gobiernos, ahora es una diplomacia que implica a la sociedad civil, la academia, los medios, los sectores productivos y el ciberespacio.

En el contexto de la globalización, la diplomacia ha dejado de ser una actividad exclusivamente entre Estados y se ha transformado en un proceso complejo que involucra múltiples actores, canales y plataformas. Lejos de operar únicamente en entornos cerrados o "clubes diplomáticos", la diplomacia del siglo XXI se desarrolla en entornos abiertos, hiperconectados y en tiempo real, donde la visibilidad, la inmediatez y la interacción ciudadana redefinen la forma en que se construyen las relaciones internacionales. (IDEAS-UNO, 2015)

La diplomacia contemporánea ha evolucionado hacia un modelo más abierto, dinámico y participativo, conocido como ciberdiplomacia, en el cual el Estado ya no actúa de manera exclusiva en la escena internacional, sino en articulación con una diversidad de actores: organizaciones

multilaterales, empresas, ciudades, ciudadanos y plataformas digitales. Este modelo reconoce que la influencia internacional se construye a través de conexiones horizontales, colaboración multiactor y la gestión estratégica de la información en tiempo real. (IDEAS-UNO, 2015)

En este escenario, los ministerios de relaciones exteriores han pasado de ser entidades centralizadas con control absoluto de la política exterior, a desempeñar un rol de coordinación dentro de sistemas interconectados y descentralizados. Las herramientas digitales —como redes sociales, blogs, bases de datos abiertas y plataformas colaborativas— se han convertido en espacios legítimos de mediación e influencia. La figura del diplomático, por tanto, también se redefine: deja de operar únicamente en círculos cerrados y pasa a formar parte activa del diálogo público global, combinando su función técnica con habilidades comunicativas, tecnológicas y estratégicas.

La ciberdiplomacia, en este contexto, emerge como la dimensión estratégica de la diplomacia moderna frente a los retos del ciberespacio. Casos recientes, como el ciberataque a Albania en 2022, atribuido a un actor estatal extranjero, o el liderazgo de Estonia y Letonia en ciberseguridad y gobernanza digital, evidencian cómo el entorno digital puede afectar directamente las relaciones exteriores y la seguridad internacional. La acción diplomática, por tanto, debe incorporar capacidades de análisis en tiempo real, respuesta estratégica a amenazas digitales, y participación activa en la configuración de normas internacionales en ciberseguridad.

La incorporación de tecnologías emergentes, como la Inteligencia Artificial (IA), representa una transformación en la manera en que el Estado organiza, analiza y utiliza la información para diseñar y ejecutar políticas. En la administración pública, la IA permite automatizar procesos, analizar grandes volúmenes de datos, predecir escenarios y tomar decisiones informadas de manera más eficiente (Brynjolfsson & McAfee, 2017).

La adopción estratégica y responsable de tecnologías emergentes, especialmente la Inteligencia Artificial (IA), está redefiniendo el rol del Estado en América Latina y el Caribe. En el contexto de la gestión pública, la IA tiene el potencial de transformar la formulación de políticas, la eficiencia operativa y la transparencia institucional, siempre que se acompañe de marcos éticos, capacidades técnicas e infraestructura adecuada. En el caso de la política exterior, estas tecnologías pueden aplicarse al análisis geopolítico, la anticipación de escenarios, la sistematización de datos diplomáticos y la detección de amenazas digitales. La adopción de IA no debe ser únicamente operativa, sino estratégica, como catalizadora de una diplomacia más informada, preventiva e innovadora. (OECD/CAF, 2022).

El desarrollo normativo colombiano en seguridad digital y su vínculo con la diplomacia, en junio 2025, Colombia adoptó la *Estrategia Nacional de Seguridad Digital 2025–2027*, con el propósito de consolidar un entorno digital seguro, resiliente y centrado en la protección de los derechos ciudadanos. Esta política responde al aumento de amenazas en el ciberespacio: en 2024, el país registró aproximadamente 36.000 millones de intentos de ataque, siendo el segundo más afectado de América Latina (Ministerio TIC, 2025).

La estrategia se basa en cuatro pilares: gobernanza digital, ciber resiliencia, fortalecimiento del talento digital y actualización normativa. Aunque representa un avance significativo en ciberseguridad, no contempla una articulación explícita con la política exterior ni con la Cancillería, omitiendo el enfoque de la ciberdiplomacia. Esta ausencia evidencia una brecha entre la gestión de riesgos digitales internos y la proyección internacional del país.

Desde el ámbito diplomático, esto puede abordarse como una oportunidad para fortalecer el rol del Ministerio de Relaciones Exteriores en escenarios multilaterales. Integrar la dimensión

internacional en la estrategia permitiría a Colombia anticipar riesgos transnacionales, participar en la construcción de normas globales y posicionarse como referente regional en diplomacia digital.

Planteamiento conceptual

Elemento	**Descripción**
Nombre del producto	Estrategia de preparación institucional en ciberdiplomacia para el Ministerio de Relaciones Exteriores de Colombia.
Objetivo general	Fortalecer las capacidades institucionales del Ministerio para anticiparse y responder a riesgos digitales que afecten la política exterior.
Justificación	La creciente digitalización de la diplomacia y las amenazas cibernéticas requieren que la Cancillería avance hacia una gestión preventiva y prospectiva.
Antecedentes clave	Casos de Estonia (ciberataque y liderazgo digital), Albania (ciberdiplomacia reactiva) y Letonia (cooperación digital y resiliencia diplomática).
Ámbitos de acción propuestos	✓ Sensibilización institucional: Difundir boletines mensuales sobre ciber amenazas y diplomacia; realizar ejercicios simulados de respuesta ante incidentes digitales; e

	impulsar campañas internas sobre cultura de ciberseguridad. ✓ Formación técnica: Ofrecer capacitaciones en ciberdiplomacia y geopolítica digital, complementadas con un curso virtual básico para funcionarios nuevos. ✓ Coordinación interinstitucional: Crear un grupo de trabajo con MinTIC y la Agencia Nacional Digital para monitorear riesgos digitales y coordinar acciones; establecer lazos con organismos multilaterales en ciberseguridad. ✓ Participación internacional: Impulsar la presencia activa de Colombia en foros sobre ciberseguridad como la ONU.
Alcance institucional	Planta interna Ministerio de Relaciones Exteriores.
Limitaciones	Se trata de un marco conceptual. No implica la implementación directa de un sistema digital, pero sirve como base para procesos posteriores.
Beneficios esperados	✓ Mayor conciencia institucional sobre ciberdiplomacia.

	✓ Propuesta de lineamientos iniciales de preparación.
Valor agregado	Inicia una reflexión institucional en torno a la diplomacia digital desde una perspectiva de prevención, seguridad y gobernanza estratégica.

Tabla 1. Planteamiento conceptual del producto final.

Diagnóstico institucional

La creciente digitalización del entorno internacional ha transformado profundamente las dinámicas de la política exterior, exigiendo que entidades como el Ministerio de Relaciones Exteriores de Colombia desarrollen capacidades específicas para enfrentar riesgos emergentes del ciberespacio. No obstante, un análisis inicial de la situación interna evidencia que la ciberdiplomacia aún no se encuentra plenamente integrada como componente estratégico en la estructura institucional, lo que representa tanto un reto como una oportunidad para su fortalecimiento.

Fortalezas (F)	**Debilidades (D)**
• Interés institucional emergente en temas de diplomacia digital, expresado en espacios como el GIT. • Presencia de herramientas digitales como SharePoint y Copilot que pueden ser optimizadas.	• Ausencia de una política institucional o protocolo específico sobre ciberdiplomacia. • La alta rotación de personal limita la continuidad del conocimiento institucional y evidencia la falta de procedimientos estandarizados que

• Experiencia del Ministerio en relaciones multilaterales, clave para espacios de gobernanza digital. • Capacidad de articulación interinstitucional con sectores como defensa, ciencia y tecnología.	garanticen la transferencia efectiva de información. • Escasa sistematización estratégica de información diplomática y seguimiento a riesgos digitales. • Falta de formación especializada en temas de ciberseguridad e inteligencia digital.
Oportunidades (O)	**Amenazas (A)**
• Casos de países como Estonia, Albania y Letonia ofrecen referentes y modelos aplicables a Colombia. • Mayor interés global por establecer normas de conducta estatal en el ciberespacio (ONU, UE, OSCE). • Posibilidad de posicionar a Colombia como actor responsable e innovador en escenarios multilaterales. • Avance de la inteligencia artificial como catalizador para la gestión diplomática y la anticipación.	• Aumento global de ciberataques dirigidos a entidades estatales, incluidas las diplomáticas. • Riesgo de afectar relaciones bilaterales si Colombia no cuenta con capacidad de respuesta adecuada. • Fragmentación del ciberespacio y tensiones geopolíticas entre potencias tecnológicas. • Vulnerabilidad de sistemas informáticos en misiones y sedes diplomáticas ante ataques o filtraciones.

Tabla 2. Análisis FODA.

En la entrevista realizada a Daniel Rodríguez, tercer secretario del Ministerio que participó en una misión técnica en ciberseguridad y diplomacia digital en Estonia (comunicación personal, 4 de agosto de 2025). La entrevista tuvo como objetivo conocer percepciones y aprendizajes sobre la experiencia de Estonia en ciberseguridad, así como evaluar la aplicabilidad de sus modelos al contexto colombiano. A continuación, se presentan algunos fragmentos clave:

Pregunta 1: *¿Cuáles considera que son los principales aprendizajes institucionales del caso estonio aplicables a Colombia?* Respuesta: "Lo más destacable de Estonia es su enfoque sistémico. Tienen una arquitectura de seguridad digital que combina liderazgo político, normativa clara, cooperación interinstitucional y capacitación continua. En Colombia, aún nos falta integrar la ciberseguridad como un componente estratégico de la política exterior, más allá de los temas técnicos del MinTIC".

Pregunta 2: *¿Cómo evalúa la preparación institucional actual del Ministerio en materia de ciberdiplomacia?* Respuesta: "Desde mi experiencia, en el Ministerio este tema aún es nuevo. Hay interés, pero no hay una estrategia clara ni personal formado específicamente en estos temas."

Pregunta 3: *¿Qué buenas prácticas observadas en Estonia podrían implementarse en el GIT de Europa Occidental?* Respuesta: "Una de las prácticas más replicables es la creación de *Cyber Ranges*, espacios de simulación y formación para funcionarios públicos. También la integración de indicadores de ciberseguridad en los perfiles-país, lo que permite anticipar riesgos geopolíticos emergentes desde el ámbito digital".

Esta entrevista evidencia que, si bien existe un reconocimiento creciente de la importancia de la ciberseguridad en el ámbito diplomático, persisten vacíos institucionales significativos en

términos de formación, normatividad, articulación interinstitucional y gestión estratégica de información.

Resultados

A lo largo del desarrollo de la práctica profesional, se identificaron tres hallazgos clave:

1. Una brecha institucional en materia de ciberdiplomacia, en la cual el Ministerio de Relaciones Exteriores de Colombia carece actualmente de una estrategia formal o lineamientos técnicos en ciberdiplomacia. Esta ausencia representa una limitación significativa en un contexto internacional marcado por crecientes amenazas cibernéticas y dinámicas de gobernanza digital. La falta de preparación institucional puede comprometer la capacidad de respuesta ante incidentes en el ciberespacio y debilitar la proyección internacional del país en asuntos tecnológicos.

2. La propuesta conceptual para la preparación institucional como un aporte principal del ejercicio práctico, se formuló un marco conceptual que orienta a la Cancillería hacia el fortalecimiento de sus capacidades en materia de ciberdiplomacia. Esta propuesta contempla acciones como campañas de sensibilización, monitoreo de amenazas, coordinación interinstitucional y posicionamiento en foros multilaterales. El planteamiento se inspira en enfoques contemporáneos de gestión pública como la Nueva Gestión Pública, el Gobierno Abierto y la diplomacia en red, y no implica requerimientos tecnológicos inmediatos, sino más bien una reestructuración estratégica de procesos.

3. Una evaluación institucional mediante el diagnóstico estratégico, en el cual se utilizó la matriz FODA como herramienta de análisis para caracterizar el estado actual de la Cancillería frente a los desafíos digitales. Entre las fortalezas se destaca el creciente interés en el tema y la trayectoria diplomática del personal; entre las debilidades, la baja

sistematización de información, la limitada formación en ciberseguridad y la falta de procedimientos estandarizados. Se identificaron también amenazas externas como el aumento global de ataques digitales a servicios exteriores y la pérdida de liderazgo internacional si no se desarrollan capacidades en esta materia.

En conclusión, el análisis evidencia la necesidad urgente de avanzar hacia una preparación institucional más sólida en seguridad digital y diplomacia tecnológica, articulando los desarrollos normativos nacionales con una política exterior proactiva frente a los retos del entorno digital.

Análisis prospectivo.

En un entorno internacional cada vez más condicionado por el avance de la digitalización y la intensificación de amenazas transnacionales en el ciberespacio, resulta fundamental que la Cancillería colombiana adopte una visión prospectiva que le permita anticiparse a los posibles escenarios futuros. La técnica de los ejes de Schwartz ofrece una herramienta metodológica útil para visualizar y contrastar diferentes futuros posibles, a partir de la combinación de dos variables críticas: el nivel de institucionalización de la ciberdiplomacia en el Ministerio de Relaciones Exteriores y el nivel de conflictividad digital en el entorno internacional.

Ambas variables presentan un alto grado de incertidumbre, pero resultan esenciales para definir la capacidad del Estado colombiano de ejercer una política exterior proactiva, resiliente y coherente con los desafíos del siglo XXI. Con base en esta matriz, se proyectan cuatro escenarios posibles, cada uno con implicaciones distintas para el desempeño institucional de la Cancillería:

Escenario 4 – Vulnerabilidad crítica	**Escenario 1 – Liderazgo estratégico digital**
En un escenario de alta amenaza y baja preparación, Colombia enfrenta impactos	Colombia se anticipa a los cambios y consolida su papel en foros globales,

negativos sobre su legitimidad internacional y su seguridad diplomática.	integrando la ciberdiplomacia en su estructura institucional.
Escenario 3 - Oportunidad no aprovechada	**Escenario 2 – Fortaleza resiliente**
Aunque el entorno es relativamente estable, la inacción institucional limita el posicionamiento y la adaptación del país.	Ante un entorno de alta amenaza, el país responde con capacidades robustas y alianzas internacionales.

Tabla 3. Ejes de Schwartz.

Esta reflexión no pretende predecir el futuro, sino ofrecer un marco estratégico de análisis que permita tomar decisiones informadas, fortalecer capacidades institucionales y orientar el diseño de políticas públicas en materia de diplomacia digital.

Recomendaciones

1. Incorporar la ciberdiplomacia como una línea transversal de trabajo en la política exterior colombiana, adaptando las estructuras existentes del Ministerio a los desafíos del entorno digital.
2. Fomentar alianzas estratégicas con actores clave, como MinTIC, la Agencia Nacional Digital, la OEA y la Unión Europea, para identificar experiencias compartidas y coordinar acciones ante riesgos cibernéticos.
3. Establecer una unidad técnica especializada en diplomacia digital, encargada de monitorear amenazas internacionales, sistematizar información y representar a Colombia en foros globales sobre ciberseguridad.
4. Diseñar e implementar programas de formación continua, dirigidos a funcionarios de planta y contratistas, en temas como seguridad digital, geopolítica de la tecnología y diplomacia multicanal.

5. Actualizar el reglamento interno del Ministerio en materia digital, incluyendo protocolos de ciberseguridad, uso de tecnologías emergentes y estándares éticos para el uso institucional de inteligencia artificial.
6. Promover una cultura organizacional de prevención, a través de campañas internas de sensibilización, simulacros de cibercrisis y espacios colaborativos para el análisis de escenarios futuros.

Conclusiones

La acelerada transformación digital del entorno internacional ha generado nuevos retos para la política exterior colombiana, particularmente en lo referente a la seguridad digital, la protección de infraestructuras críticas y la diplomacia en entornos tecnológicos complejos.

El Ministerio de Relaciones Exteriores, como actor clave en la representación y proyección del Estado, debe fortalecer su capacidad institucional para anticipar y gestionar amenazas provenientes del ciberespacio, integrando la perspectiva de ciberdiplomacia en sus estrategias y estructuras operativas. Si bien la Estrategia Nacional de Seguridad Digital 2025–2027 establece una hoja de ruta para el país, su implementación efectiva requiere que el Ministerio participe en la definición de protocolos de acción exterior y diplomacia digital en la entidad.

Finalmente, la propuesta formulada se orienta a anticipar, mitigar y gestionar riesgos digitales que inciden directamente en la política exterior colombiana. Al fortalecer la sensibilización interna, la formación técnica, la coordinación interinstitucional, la gestión estratégica de la información y la participación en foros internacionales, el Ministerio de Relaciones Exteriores estaría en capacidad de responder de manera más ágil y efectiva a las amenazas del ciberespacio. Estos lineamientos, además de proteger la seguridad de la información

diplomática, buscan resguardar la imagen del Estado en el exterior y consolidar un rol proactivo en la gobernanza internacional del ciberespacio, contribuyendo al posicionamiento de Colombia como un actor responsable, resiliente y comprometido con la cooperación digital.

Bibliografía

Brynjolfsson, E., & McAfee, A. (2017). *Machine, Platform, Crowd: Harnessing Our Digital Future.* W. W. Norton & Company.

Christou, G. (2015). *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy (New Security Challenges).* Palgrave Macmillan.

CLAD, C. L. (1998). *Una Nueva Gestión Pública para América Latina.* CLAD, Centro Latinoamericano de Administración para el Desarrollo.

IDEAS-UNO. (2015). Diplomacia y gobernanza global. *Revista IDEAS, Naciones Unidas.*, 2.

Kavanagh, J. (2022). *The Albania-Iran cyberattack: Lessons in diplomatic response.* Carnegie Endowment for International Peace.

Kurbalija, J. (2016). *An Introduction to Internet Governance.* DiploFoundation.

Melissen, J. (2005). The New Public Diplomacy: Between Theory and Practice. En J. Melissen, *The New Public Diplomacy, Soft Power in International Relations* (págs. 3-23). New York, N.Y.: Palgrave.

Ministerio de Comercio, Industria y Turismo. (2024). *Tratado de Libre Comercio entre Colombia y los Estados EFTA. .* Obtenido de Tratado de Libre Comercio entre Colombia y los Estados EFTA. : https://www.mincit.gov.co

Ministerio de las Culturas, las Artes y los Saberes de la República de Colombia. (2025). *Agenda cultural bilateral Colombia-España.* Obtenido de Agenda cultural bilateral Colombia-España: https://www.mincultura.gov.co

Ministerio de Relaciones Exteriores. (2025). *"Damos inicio a un proceso de fortalecimiento con la Unión Europea": Canciller Laura Sarabia cierra agenda de alto nivel en Bruselas.* Bogotá: Ministerio de Relaciones Exteriores.

Ministerio de Relaciones Exteriores. (2025). *Asuntos políticos, económicos, culturales, educativos, ciencia y seguridad temas de interés durante la Reunión de Consultas Políticas entre Colombia y Francia.* Bogota: Ministerio de Relaciones Exteriores.

Ministerio de Relaciones Exteriores. (2025). *Colombia e Irlanda participaron en la III reunión de consultas políticas.* Bogota: Ministerio de Relaciones Exteriores. Obtenido de Ministerio de Relaciones Exteriores: https://www.cancilleria.gov.co/newsroom/news/colombia-e-irlanda-participaron-iii-reunion-consultas-politicas

Ministerio de Relaciones Exteriores de Colombia. (2024). *Manual de funciones y competencias laborales.* . Obtenido de Manual de funciones y competencias laborales. : https://www.cancilleria.gov.co

Ministerio de Relaciones Exteriores. (2016). *Decreto 869 de 2016: Por el cual se establece la estructura del Ministerio de Relaciones Exteriores.* . Bogotá D.C.: Ministerio de Relaciones Exteriores. .

Ministry of Foreign of Republic of Estonia. (2024). *Cybersecurity Strategy 2024–2030 'Cyber-Conscious Estonia'.* Obtenido de Ministry of Foreign of Republic of Estonia: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/EE_NCSS_2024_en.pdf

Nye, J. S. (2010). *Cyber Power.* Harvard Kennedy School - Belfer Center for Science and International Affairs.

Ocampo, J. A. (2015). *Gobernanza global y desarrollo: Nuevos desafíos y prioridades de la cooperación internacional.* . Siglo Veintiuno Editores.

OCDE, O. p. (2015). *Gobierno Abierto en América Latina, Estudios de la OCDE sobre Gobernanza Pública.* OECD.

OECD/CAF. (2022). *The strategic and responsible use of artificial intelligence in the public sector of Latin America and the Caribbean.* . OECD Public Governance Reviews.

Organización para la Cooperación y el Desarrollo Económico. (2022). *Evaluación de la gobernanza pública en Colombia.* Obtenido de Evaluación de la gobernanza pública en Colombia.: https://www.oecd.org

Osborne, D. (1992). Reinventing Government. *League for Innovation in the Community Coll.*

Oszlak, O. (2013). Gobierno abierto: hacia un nuevo paradigma de gestión pública. *Red de Gobierno Electrónico de América Latina y el Caribe*, 1-35.

Unión Europea. (2023). *Relaciones Unión Europea-Colombia: Informe de cooperación* . Obtenido de Relaciones Unión Europea-Colombia: Informe de cooperación : https://eeas.europa.eu

Wilson, J., & Daugherty, P. (July de 2018). Collaborative Intelligence: Humans and AI Are Joining Forces. *Harvard Business Review*.